Information Security and Privacy Advisory Board (ISPAB)

Summary of Meeting

George Washington University
Cafritz Conference Center
800 21st Street, Room 413-414
Washington DC

June 7 - 8, 2007

June 7, 2007

Board members attending in person were Dan Chenok, Brian Gouker, Joseph Guirreri, Susan Landau, Rebecca Leng, Lynn McNulty, Alexander Popowycz, Leslie Reis, Philip Reitinger, Jaren Doherty, Fred Schneider, and Pauline Bowen as the Designated Federal Official. Dan Chenok chaired the meeting and board members introduced themselves and reported on their current activities. Dan Chenok explained the absences of Lisa Schlosser, who was called up to serve as reserve, while Howard Schmidt was attending to personal business. Throughout the 2-day meeting, various members provided refreshments and snacks. NIST attendees included Dr. Jim Turner, the new Deputy Director, Cita M. Furlani, Director, Information Technology Laboratory (ITL), Jim St. Pierre, Deputy Director, ITL, Curt Barker, Division Chief, Computer Security Division (CSD), Donna Dodson, Deputy Division Chief (CSD), and Liz Chew, Group Manager (CSD). Note was taken by Annie Sokol, NIST.

Dan Chenok elaborated on each agenda items for this meeting. Lynn McNulty discussed progress on the "Essential Body of Knowledge" for cybersecurity professionals. Rebecca Leng noted that IGs are gearing up for FISMA reviews. The Board raised the issue of quantum crypto in hope that the board members would look into this issue and other issues relating to this subject. Rebecca Leng would like to know if Dan Chenok still plans to talk to IG communities in the forthcoming months, and whether the board has any suggestions for the IG communities. Dan said he would attend.

NIST Briefing/

Cita Furlani introduced Dr. James Turner, the new Deputy Director of National Institute of Standards and Technology (NIST). Prior to joining NIST on April 16, 2007, Dr. Turner served as Assistant Deputy Administrator for Nuclear Risk Reduction at the Department of Energy (Nuclear Security Administration). In addition to a PhD in Physics from MIT and a Bachelor's in Physics from Johns Hopkins University, Jim spent five years as an Associate Professor of Physics and Engineering at Morehouse College and has almost 20 years experience as a Senior Executive in the Federal Government. He has won numerous awards for his government service including the Presidential Rank Award for Meritorious Service.

Dr. Turner briefed the board on NIST, including an overview of the setup, goals, challenges, programs, profile, an overview of appropriated funding for NIST for 2007, and NIST's request for FY2008. Dr Turner noted that NIST activities need to be premised on a balancing of security, cost, and usability – higher security that drives risk down is less efficient, considering trade-offs is important. Information security is an element of each part of NIST's labs, so it has a high degree of importance for Dr. Turner. In response to Susan Landau's point that NIST actions are often not widely disseminated in forms understandable to the nontechnical executive,, Dr. Turner provided examples from NIST's current or planned information security work which the board is actively involved. Rebecca Leng pointed out that FISMA was developed in 2001, is far from fully efficient in its implementation, and it has yet to work out all issues – including how to balance the role of the IG in assessing compliance with the need for transparency.

Curt Barker gave a presentation on the status of CSD Activities. He explained the mission goals are to provide standards and technology to protect information so as to build trust and confidence in Information Technology (IT) systems. He also addressed threats and challenges. Curt Barker further stated that program managers are working on metrics within certain characterization issues, and a coordination program focusing on cyber security metrics that would be fleshed out over the next 3-6 months. He reported the following – 1) SP 800-53A 3rd draft has been issued and it is presently gathering comments; 2) NIST is looking at how to reduce costs for C&As, and 3) SP104 on HSPD 12 is in final consensus and under refinement. The board will decide whether to be involved in submitting comments on the third draft of SP 800-53A. The Board also noted that NIST could bring clarity by addressing the needs of system owners separately from central network owners. Distributed Identification and Protection of Citizen Data Panel

Alex Popowycz, Fidelity (chair), VP, Information security
Robin Wilton, Corporate Architect, Sun Microsystems
Peter Lord, Director, Technology Policy, Oracle
Khaja Ahmed, Architect, Windows Networking Security, Microsoft

Bios:

Robin Wilton, Corporate Architect, Federated Identity, and Chief Technology Office, Business Alliances, Sun Microsystems
Having recently joined the Business Alliances team of Sun's Chief Technology Office, Robin Wilton, is part of a team whose role is to look outwards (at Sun's relationships with strategic business partners) and inwards across the Sun product lines – seeking to maximize Sun's added value in all areas of identity management through business innovation. In his five years at Sun Microsystems have included EMEA technical pre-sales responsibility for the Directory, Meta-directory, Certificate Manager and Trustbase products, and EMEA Programme Manager for the Java Desktop System, Wilton has also undertaken consulting engagements for Sun's customers in the investment banking sector. Among other roles, he worked in IBM Technical Support on retail banking and cryptographic hardware products. As well as consulting engagements in the UK, Argentina and Turkey, he delivered a course on IBM's Key Management system to the Central Bank of Russia in Irkutsk. In his consulting role, he undertook a security audit of the messaging security system for the London Stock Exchange. Mr. Wilton has also written and delivered a number of training courses to colleagues, customers and partners, on banking products, security and key management.

Peter Lord is Director of Technology Policy for Oracle where he advises on issues related to the intersection of technology, business, and public policy. Current areas of engagement are open standards, open source, privacy and information security policy. Prior to this role, Peter served as Oracle's Senior Manager for Global Trade Compliance. Before joining Oracle, he worked for U.S. Senator Olympia Snowe. A graduate of Bowdoin College, Peter is a Masters candidate at Georgetown University.

Khaja Ahmed is currently the Architect of Microsoft's .NET Passport service as well as head of security for MSN's MPG (Member Platform Group). In his role as head of security for MPG Khaja manages the security for all of MSN's authentication (Passport), billing, Digital Micro Payments, and other security critical services. As Architect of Passport, he is responsible for the architecture of the Identity Management and authentication service for all MSN and partner services. He is also Microsoft's representative on the Electronic Authentication Council which is working on authentication solution for eGovernment services. Khaja has been in the domain of information security since 1990 and in the computer Industry since 1986. He is actively involved in the development of security standards (within and outside of Microsoft) that encompass management of Identities and their attributes. Over the last dozen plus years he has been involved in designing, implementing and integrating a range of security solutions and services for fortune 500 companies, Financial Institutions, Healthcare as well as various security sensitive departments of the US Federal Government and other countries.

The security technologies and solutions he has worked on include PKI, virtual and physical tokens, Crypto Accelerators, key management systems, trusted operating systems / trusted platforms, Intrusion detection systems, Audit and vulnerability assessment tools, secure communication protocols, bio-metric devices, mobile security solutions, Identity management systems, Authorization systems, etc.

Summary:

The panel was assembled and chaired by Alex Popowycz, to inform the board about considerations and in using distributed identification methods for the public sector, and to provide information about on-going efforts in deploying distributed identity systems for citizen services. The panel also elaborated on happenings in the industry, and touched on how government and other entities handle ID protection. Generally, there is an over-simplification on the use of identity and a lot of information on the web which people are unable to access. There is a need to have a federated set-up similar to Liberty Alliance, which offers a global identity management solution.

Liberty Alliance is set up with to enable networks based on open standards, business and deployment guidelines and best practices for managing privacy, where consumers, citizens, businesses and governments can more easily conduct online transactions while protecting the privacy and security of identity information.

The panel also discussed a SOA-based approach to id management, designed around provisioning government services to those who need them for performing activities related to a given service. Factors in the take-up to this approach include privacy, security, efficiency, cost, and trust in government. Privacy was identified as a key risk – identity management systems can require that too many attributes be provided to complete a transaction, rather than tailoring the attribute to a policy that minimizes data collected (e.g., many transactions can be done anonymously).

The panel discussed whether the US government should impose a uniform protocol for all users -- i.e. responsible parties in the industry, various governments, NGOs, quasi-governmental bodies, and standards bodies -- in acquiring and using data so that there will be transparency, vulnerability protection and control for identity and privacy with a common user experience (meaning the manner in which users interact with the identity management systems. It is necessary to first define non-technical aspect of identity data, so as to design a workable solution for government that includes a system that will eliminate the inconvenience for accessing identity data. Ultimately, governments will likely have multiple solutions, but these could be arrived at through an inclusive process that focuses on principles of interoperability. Phil Reitinger recommended that the Board review the work of the NSTAC Identity Management Task Force.

NRC Privacy Study
Herb Lin, NRC/CSTB

Bio:

Dr. Herbert Lin is senior scientist and senior staff officer at the Computer Science and Telecommunications Board, National Research Council of the National Academies, where he has been study director of major projects on public policy and information technology. These studies include a 1996 study on national cryptography policy (*Cryptography's Role in Securing the Information Society*), a 1991 study on the future of computer science (*Computing the Future*), a 1999 study of Defense Department systems for command, control, communications, computing, and intelligence (*Realizing the Potential of C4I: Fundamental Challenges*), a 2000 study on workforce issues in high-technology (*Building a Workforce for the Information Economy*), a 2002 study on protecting kids from Internet pornography and sexual exploitation (*Youth, Pornography, and the Internet*), a 2004 study on aspects of the FBI's information technology modernization program (*A Review of the FBI's Trilogy IT Modernization Program*), a 2005 study on electronic voting (*Asking the Right Questions About Electronic Voting*), and a 2005 study on computational biology (*Catalyzing Inquiry at the Interface of Computing and Biology*).

Prior to his NRC service, he was a professional staff member and staff scientist for the House Armed Services Committee (1986-1990), where his portfolio included defense policy and arms control issues. He received his doctorate in physics from MIT.

Dr. Lin is presently working on the following projects: 1) Engaging the Computer Science Research Community in Health Care Informatics, 2) Policy Consequences and Legal/Ethical Implications of Offensive Information Warfare, 3) Information for Terrorism Prevention and Other National Goals, and 4) Cybersecurity Research in the United States. The board invited Dr. Lin to discuss the NRCs cybersecurity research report, which has been cleared the in-house review process, and moving on to prepublication form. This stage entails at least one round of editing to make sure that any existing ambiguities have been clarified. Presently, NRC is trying to organize a briefing for all report sponsors with this prepublication version.

Dr. Lin as one of the authors of *Engaging Privacy and Information Technology in a Digital Age*, explained that the research report is to provide ways of thinking about privacy and its relationship to other values and related tradeoffs; and consider IT trends as related to privacy concerns. The report focused on the fundamental concepts of privacy, laws surrounding privacy, the trade-offs in societally important areas, and the impact of technology on conceptions of privacy. The key concepts were based on the following:

- Personal Information, Sensitive Information, and Personally Identifiable Information
- False positives, False Negatives, and Data Quality
- Privacy and Anonymity
- Fair Information Practices
- Reasonable Expectations of Privacy

Summary:

Herb Lin provided the findings and recommendations specifically for organization and policy makers. Herb indicated that the NRC looked at a broad range of privacy and information issues. They observed that incremental change is best in this area, due more to the complexity of the issue than political feasibility. The spirit of existing law is key and should be respected. The Committee's recommendations included improvements in PIAs, enforcement, and redress, as well as an institutional advocate role for privacy. The Board and Herb discussed several challenges, including:

- application of fair information principles across the private sector
- providing clarity in how information is "repurposed" (is it the initial creator or the redisclising entity who should provide notice?
- choice and consent – need to move beyond opt-in and opt-out.
- Government's coercive power makes it especially important to assess privacy implications of technology trends, such as MySpace for government.
- Potentially, the need for a national Privacy Commissioner.

Susan Landau asked what was the most important finding, for which Herb Lin stressed that the answer required further analysis. He stressed that the key findings and recommendations included in the report are inclusive and good enough to be submitted to the government for consideration.

<u>GAO Privacy Study</u>
John A de Ferrari, Assistant Director, IT, GAO

John de Ferrari presented the rationale for the review of privacy laws with the following parameters:

- GAO has recently initiated a review of the adequacy of the Privacy Act of 1974, the E-Government Act of 2002, and related guidance in light of contemporary practices for acquiring, managing, analyzing, and sharing personal information.
- GAO's review is currently in the first of two phases, called the "design" phase.
- The design phase will continue until the end of July 2007.

- A target date for a final report has not yet been determined.

He further supported his presentation with design phase objectives, methodologies, and a list of other recent reports on privacy. It is unlikely that this study will conclude before the end of this fiscal year.

The GAO study was requested after the VA data breach GAO is reviewing many existing materials, including past GAO reports and the OECD Fair Information Principles, as inputs.

Software Configuration Panel
Dan Mintz, CIO, Department of Transportation
Dan Costello, Senior Policy Analyst, OMB
Ken Heitkamp, DoD
Jaren Doherty, Department of Health and Human Services

Bios:

Daniel G. Mintz became CIO of the Transportation Department in May 2006. He has over thirty years experience in industry systems prior to joining DOT. In his previous job at Sun Microsystems, Mintz was director for government compliance programs. He was responsible for any projects that Sun worked for the government aligned with federal security, legal and regulatory requirements. Additionally, in 2005, Mintz was a delegate to the White House Conference on Aging, which focused on the use of technology to support improved medical delivery and the special issues of senior citizens. Mintz earned his bachelor's degree from the University of Maryland and has a master's degree in international management from the school's University College.

Kenneth B. Heitkamp is the Assistant Air Force Chief Information Officer for Life-Cycle Management (AF-CIO/L), Washington, D.C. He is responsible for ensuring Air Force information technology life-cycle management programs, projects, policies, and performance measures are developed in accordance with Federal, DoD and USAF guidance, policy, architecture and standards. He coordinates strategic direction and maintains oversight of major IT lifecycle management initiatives such as the Air Force IT Commodity Council (ITCC).

Summary:

The discussion began with reference to the memorandum from Karen Evans on the subject, "Managing Security Risk by Using Common Security Configuration." The panel maintained that there is no good configuration program available at this point, and it is necessary for public-private collaboration to bring about a configuration baseline and maintain a security system. Without a standardized configuration, migration to new operating systems may be ineffective.

Each agency will develop a governance structure, and can deviate up in their level of security from the baseline so long as the baseline is standardized. The panel observed that NIST continues to be a valuable resource for government agencies in implementing this memorandum.

It is possible to build a variation based on NIST baseline level of security. This core baseline level of security should then be recommended to all agencies while allowing agencies to make the final selection. This determination for a recommended baseline configuration is focused on reducing risks from security threats and vulnerabilities, saving time and resources. Contractor and other systems will have to be compatible.

Ken Heitkamp gave a presentation on how Air Force Progress in implementation Standard desktop configuration via conference call. He explained the steps taken to secure the layers of standard desktop configuration (SDC). These steps and datelines are followed as mandated by OMB's requirements. The rollout of the SDC has been agreed upon by various agencies with rigorous test configurations to identify adverse effects on system functionality. The earliest timeframe for mandatory USAF Vista use is early

2009. The Air Force has submitted a three-part clause to the DOD chief information officer that would be included in every IT contract. Eventually, DOD's rule could be given to OMB for them to decide whether to take it governmentwide. The long-term goal for the Air Force is to have real-time standard configuration management. According to Heitkamp, presently, Air Force software ensures that a laptop or PC connected to the network checks the standard configuration every 90 minutes. The service hopes to have the real-time enforcement running by 2008. Dan Chenok asked Ken Heitkamp to pass on any additional and related information to NIST.

Dan Mintz stated that DOT is at least 1-2 years away from the process described by Ken Heitkamp, and he further stated that his division lacks resources to fully monitor the system. It is critical to integrate the correct language for acquisition and implementation of policies.

Dan Costello indicated that OMB is working to incorporate standard desktop configuration requirements into federal acquisition regulations. The move should help give acquisition officials and program managers more consistent guidance on security issues, such as the incorporation of provisions of FISMA.

The Board raised several concerns with the policy:

- Security vulnerabilities that could be exacerbated by "monoculture". The panel responded that OMB felt the benefits from standard configurations would outweigh the chance of viral spread, though did not have data to support this view.
- Telecommuters and security. As more government users plug in from home machines, their desktops may not be on the standard configuration and thus may introduce new operational or security risks. The Board agreed to look into this issue more in an upcoming meeting.

General Work Plan Discussion

Dan Chenok asked for a motion that the draft Summary of the Meeting from March 22-23, 2007 be approved. Lynn McNulty proposed the Meeting Summary be approved and accepted, which was seconded by board members.

Discussion on the draft Real ID Letter
Discussion generated by Lynn on whether a general statement pertaining to requirement of encryption in order to protect any readable form of the data. (Ref. DHS real id proposed letter, p31) It is necessary to first define an opinion of the integrity of the data to recommend encryption be required.

It is difficult to comments on this proposed letter without truly knowing the perimeter of the data included in the REAL ID. Phil Reitinger was asked to research and review the proposed letter so as to present his findings to the board for next day's discussion. Dan will email the latest version of the draft letter to OMB Principal.

June 8, 2007

The Board members attending in person Dan Chenok, Brian Gouker, Joseph Guirreri, Susan Landau, Rebecca Leng, Alexander Popowycz, Leslie Reis, Philip Reitinger, Fred Schneider, and Pauline Bowen as the Designated Federal Official.

Phil Reitinger reviewed the paper on DHS REAL ID relating to encryption, and prepared a draft for review. The board edited the draft to capture the overall concept of the issue. The draft was approved and accepted by the board to be sent as a letter to OMB, with a copy to the Department of Homeland Security.

Dan Chenok proceeded to review if there were any issues from yesterday's discussion that would require action. Susan Landau suggested to invite Curt Barker, Computer Security Division, NIST, to the next meeting, so as to further clarify on yesterday's presentation, and perhaps Curt Barker would stay to interact with the board members.

Dan acknowledged the presence of Donna Dodson, Computer Security Division, NIST, thereby ensued discussion on the roles and responsibilities of this advisory board, and how the board is to work with NIST in fulfilling the board's purposes and goals. Donna Dodson will work with Pauline Bowen to address the board's needs. Dan Chenok requested the board members to submit any area of concerns to be discussed with NIST.

Fred Schneider injected that there was insufficient details and substantial groundwork on the agenda items to justify discussion and to allow the board to make any strategic actions.

Considering the amount of time the board spent on discussing privacy, Fred Schneider suggested expanding the scope to include identity protection. He also commented that the various panels on yesterday's discussion did not conclusively define the areas of concerns, and in fact, provided different issues – the Board could provide a valuable contribution by bringing clarity to the issue. Dan Chenok agreed that the board needs to agree on a set of activities based on the information presented by panelists and information discussed. Rebecca Leng suggested that the board to identify gaps and issues so as to advise OMB to prioritize on the critical areas for implementation.

Software configuration memo – there was a lengthy discussion about the mono culture standard and the impact of telecommuting. Rebecca Leng recommended that the board to identify if there are any problematic or incomplete government procedures.

Options for better security through Improved Compliance and Reporting
Ari Schwartz, Deputy Director, Center for Democracy & Technology
Glenn Schlarman, OMB Retired

Bios:

Ari Schwartz is the Deputy Director of the Center for Democracy and Technology (CDT). Schwartz's work focuses on increasing individual control over personal and public information. He promotes privacy protections in the digital age and expanding access to government information via the Internet. He regularly testifies before Congress and Executive Branch Agencies on these issues. Schwartz also leads the Anti-Spyware Coalition (ASC) , anti-spyware software companies, academics, and public interest groups dedicated to defeating spyware. In 2006, Schwartz won the RSA award for Excellence in Public Policy for his work building the ASC and other efforts against spyware.

Glenn Schlarman, who retired in December 2006, had worked in government for 34 years. Schlarman, was the Office of Management and Budget's chief of the Information Policy Branch in the Office of Regulatory Affairs, had been planning his retirement most of the year and settled on leaving after the fiscal 2008 budget season was mostly complete. He came to OMB from the Energy Department in

February 2004, replacing Dan Chenok, who moved to the private sector. Before coming to OMB, Schlarman spent time at Energy working on IT security and was an FBI analyst.

The basis of the panel centered around the questions of "How do we best measure security?" and "Who should be involved in decision making?" Ari Schwartz defined security breach. Schwartz stated that although information is restricted, access is still open to many unauthorized people. There is a wide range of standardized practices enforced by different agencies and government departments (IGs, OMB, etc.), with few standards of certification including the roles of FISMA use to standardize practices. It is up to the leadership in the government to raise the standard of awareness of privacy and security that define who will and how to put together a set of standards that will work for both government or private sectors. Ari encouraged the Board to endorse several initiatives, including:

- Best practices for Privacy Impact Assessments
- Common standards of care for information handling
- Security governance that includes CIOs and industry.

Glenn Schlarman stressed that once a standard is decided, e.g. FISMA, it is the individual agency's decision to enforce the levels of details within the standards, e.g. risk perimeter, password, etc. According to Glenn, only a third of agencies are performing well and properly. In his opinion, enforcement of compliance needs to incorporate with audit. What are the consequences of non-compliance? The individual agency is responsible for discipline for non-compliance, but that results in having the agency's budget being curtailed. GAO is responsible for the audit. The subject of accountability subsequently led to an explanation of the roles of IGs by Rebecca Leng. Government is much more transparent and therefore, the government is required to be much more accountable. The government's security compliance is equally as good as the private industry although the threshold should continue to improve. Yet, there is no standardized improvement process and government's process for disseminating standards takes too long to implement. Schlarmann also noted that FISMA is a relatively recent statute, and March 2007 represents the first full baseline.

The panelists believe that the most critical problem that the government faces today: 1) personal accountability (including for program officials who own systems), 2) dealing with consequences and defining fairness for non-compliance, 3) increasing and improving comprehensive oversight, 4) providing a basic standard of reporting, 5) implementing or improving FISMA with audit, evaluation and rigid enforcement to ensure standards for all agencies are similarly followed.

General Discussion of Priorities with the House Government Reform Staff
Adam C. Bordes, Committee on Government Reform, House of Representatives
Tony Haywood, House Government Reform (Tony Haywood is unable to attend)

Adam Bordes reported on the June 7 FISMA hearing at the House. Generally, the hearing found that FISMA is excellent model and reveals much about the systems, but it cannot completely provide the necessary measure and determine vulnerability. The committee agreed that there should be more activities in the direction of testing and evaluation criteria without additional standards, as it would be cumbersome and complicated to implement. The committee also noted that there was too much process involved in the C&A system, and not enough emphasis on quality – the government should reexamine the C&A policy going forward. There was also the concern of how to integrate procurement with configuration and security measurement without increasing budget.

Adam also reported that the quality of control of FISMA implementation across various agencies is inconsistent. Major areas of focus of the committee: 1) establish a better performance measure through implementation of a revised FISMA, 2) address integration of measurement with procurement, 3) safeguarding of personal information, and 4) oversight of managing of contractors accessing government information. There is ongoing discussion on defining the metrics with no apparent set timeframe, and it is only gathering feedback and comments. Defining the boundary of measurable is complex as it is difficult to measure the outcome even with the use of FISMA as the standards. There is no standard evaluation

program included within FISMA, and GAO is concerned that the information collected since the implementation of FISMA is either incomplete or inaccurate which will lead to serious problem in vulnerability.

The Board and Adam discussed the need for better enterprise-wide security and metrics. The Committee welcomed the ISPAB's future feedback in these areas.

Privacy Technology Project White Paper
Leslie Reis, The John Marshall Law School
Jim Harper, DHS DPIAC
Director of Information Policy Studies

Bio:

As Director of Information Policy Studies, Jim Harper focuses on the difficult problems of adapting law and policy to the unique problems of the information age. Harper is a member of the Department of Homeland Security's Data Privacy and Integrity Advisory Committee. He holds a J.D. from Hastings College of the Law.

Summary:

Leslie Reis and Jim Harper provided a brief update on the progress of this project – value added proposition, 2-step methodology to assess the regulatory framework and research, and they are working on the structure which includes the overall 'big picture". Jim Harper proceeded to provide a framework of the structure that has been released by the DPIAC, including definition of Privacy, Control, Fairness, Personal Security, Liberty, and Seclusion. Leslie will oversee work to examine past policies/statues against these and similar values.

This white paper is not intended as recommendation towards legislation. GAO is looking at this, while Leslie and company are examining what privacy laws or policies may need updating to retain adherence to commonly accepted privacy principles in light of changing technology.

The board would like to review a draft general outline as soon as possible prior to the next board meeting or before the submission which sometime around October/September. Then, the board will decide whether to sign off strictly as a white paper (10-15 pages of Executive Summary) or inclusion of all citations. Leslie Reis planned to have the paper in a standardized format, which will be uploaded in a secured website for review by the board members.

General Work Plan Discussion
Board discussion on COOP Letter

The letter, in principle, stated that reasonable privacy protection is critical in contingency planning. Board members recommended that it was also appropriate to include medical information in the consideration, and to discuss the subject with related first responder before continuing with this letter. Susan Landau moved to send the letter, which was seconded by the other members.

ISPAB Work Plan Status Review
Board Members

1) FY2006 Report to Congress on Implementation of the Federal Information Security Management Act of 2002 (from OMB). There is a FISMA template used for reporting effectiveness to OMB
   - To send a letter providing the board's interpretation with the board's recommendations to NIST
   - To provide a clear and consistent measurement metrics for compliance applied by OMB to be included as part of the letter.

Pauline Bowen informed the board that Dr. Ron Ross is prepared to speak to the board on FISMA and the future plans.

2) Dan Chenok will be meeting with NIST specifically Cita M. Furlani and Curt Barker regarding budget and resources for ISPAB.
3) Pauline Bowen suggested if the board will be interested in meeting with Jim Dray, NIST, Program Manager who had been attending meetings in Norway and Portugal with regards to identity and PIV.
4) Leslie to continue working with DHS Committee on Privacy Technology white paper
5) Intern – there is no plan to have an intern to work directly with the board, though Dan will reengage with NIST.
6) NSA's briefing
   - The board to define the scope expected from NSA (best practices, processes, standards, software and technical)
   - To provide the information to Brian Gouker within the next few weeks so that he will be able to bring the appropriate presenters to the next board meeting.
   - Define applications and scientific development and general outline so that the board could then decide the next step.
7) Telecommuting to be considered for future meetings
8) Phil Reitinger requested to extend the time for each panel for discussion and questions.
9) Dan to complete letters on Real ID and COOP per Board decisions as voted on.

Potential speakers at September future meeting (to be prioritized based on Board strategic focus areas, and scheduled based on availability):

– Curt Barker, NIST, More detailed, deeper level presentation on NIST metrics and other activities
– Hilary Jaffe, OMB (Privacy)
– Sallie McDonald, NCS
– Brian Gouker, NSA, offered to talk about NSA and its services. He will also check on the availabilities of the relevant people who will be able to give presentation at the future meeting.
– Telecommuting security issues
– Clarity in identity management schemes.
– Brenda Oldfield, Brenda.oldfield@dhs.gov, 703-235-4184, to speak on DHS "Essential Body of Knowledge."
– Privacy Technology white paper update

Pauline Bowen
Board Designated Federal Official

CERTIFIED as a true and accurate summary of the meeting.

Daniel Chenok
ISPAB Board Chairman